

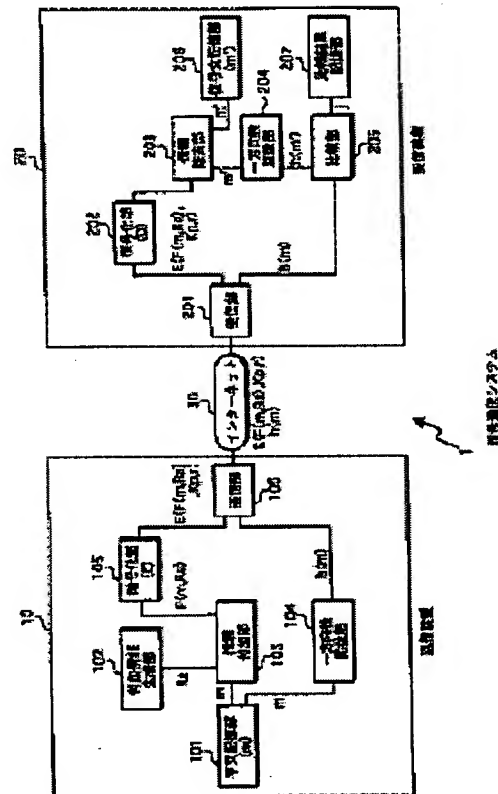
## CRYPTOGRAPHIC COMMUNICATION SYSTEM, TRANSMITTER AND RECEIVER

**Patent number:** JP2002252611  
**Publication date:** 2002-09-06  
**Inventor:** YAMAMICHI MASAHIITO; FUDA YUICHI; OMORI MOTOJI; TATEBAYASHI MAKOTO  
**Applicant:** MATSUSHITA ELECTRIC IND CO LTD  
**Classification:**  
 - international: H04L9/32; G09C1/00  
 - european:  
**Application number:** JP20010380559 20011213  
**Priority number(s):**

## Abstract of JP2002252611

**PROBLEM TO BE SOLVED:** To provide a cryptographic communication system with higher information security.

**SOLUTION:** A transmitter provides a plaintext with a one-way function to generate a first function value and first additional information, applies a reversible operation to the plaintext and the first additional information to generate joint information, and applies cryptographic algorithm to the joint information to generate a cryptogram. A receiver generates a second additional information similar to the first one, applies decoding algorithm to the cryptogram to generate decoded joint information, applies a reverse operation of the reversible operation to the decoded joint information and the second additional information to generate a decoded sentence, provides the decoded sentence with the one-way function to generate a second function value, compares the first function value with the second one, and determines the decoded sentence to be correct if these two function values agree with each other.



Data supplied from the esp@cenet database - Worldwide



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-252611

(P2002-252611A)

(43) 公開日 平成14年9月6日(2002.9.6)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

H 0 4 L 9/32

G 0 9 C 1/00

6 4 0 D 5 J 1 0 4

G 0 9 C 1/00

6 4 0

H 0 4 L 9/00

6 7 5 A

審査請求 未請求 請求項の数19 O L (全 21 頁)

(21) 出願番号 特願2001-380559(P2001-380559)

(22) 出願日 平成13年12月13日(2001.12.13)

(31) 優先権主張番号 特願2000-384835(P2000-384835)

(32) 優先日 平成12年12月19日(2000.12.19)

(33) 優先権主張国 日本(JP)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 山道 将人

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 布田 裕一

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗

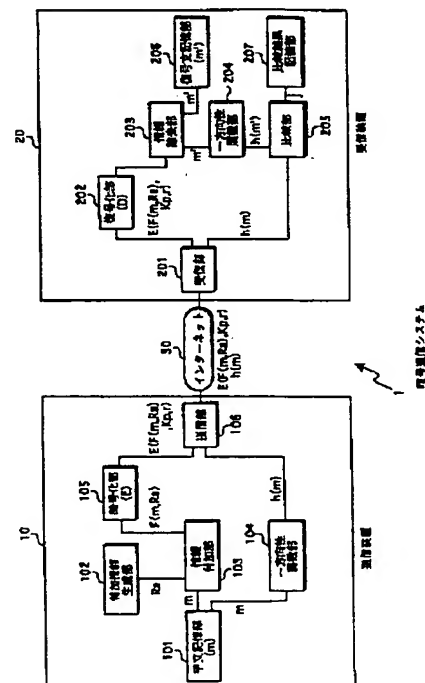
最終頁に続く

(54) 【発明の名称】 暗号通信システム、送信装置及び受信装置

(57) 【要約】

【課題】 さらに安全性の高い暗号通信システムを提供する。

【解決手段】 送信装置は、平文に一方方向性関数を施して第1関数値を生成し、第1付加情報を生成し、前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成し、前記結合情報に暗号アルゴリズムを施して暗号文を生成する。受信装置は、第1付加情報と同一の第2付加情報を生成し、前記暗号文に、復号アルゴリズムを施して復号結合情報を生成し、前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成し、復号された復号文に前記一方方向性関数を施して第2関数値を生成し、前記第1関数値と前記第2関数値とを比較し、一致する場合に復号文が正当であると判断する。



## 【特許請求の範囲】

【請求項1】 平文を暗号化して暗号文を得、前記平文に一方性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、送信装置は、  
第1付加情報を生成する第1生成手段と、  
前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、  
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、  
前記暗号文を送信する送信手段とを含み、  
受信装置は、  
前記暗号文を受信する受信手段と、  
前記第1付加情報と同一の第2付加情報を生成する第2生成手段と、  
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、  
前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含むことを特徴とする暗号通信システム。

【請求項2】 前記第1生成手段及び前記第2生成手段は、同期して、それぞれ同一内容の第1付加情報及び第2付加情報を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項3】 前記第1生成手段は、生成した前記第1付加情報を送信し、  
前記第2生成手段は、前記第1付加情報を受信し、受信した前記第1付加情報を第2付加情報とすることを特徴とする請求項1に記載の暗号通信システム。

【請求項4】 前記第1生成手段は、生成した前記第1付加情報に暗号アルゴリズムを施して、暗号化付加情報を生成して送信し、  
前記第2生成手段は、前記暗号化付加情報を受信し、受信した暗号化付加情報に前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して、付加情報を生成し、生成した付加情報を第2付加情報とすることを特徴とする請求項1に記載の暗号通信システム。

【請求項5】 前記第1生成手段は、乱数を生成し、生成した乱数を前記第1付加情報とすることを特徴とする請求項1に記載の暗号通信システム。

【請求項6】 前記可逆演算手段は、前記平文及び前記第1付加情報に、ビット結合を施して、結合情報を生成し、  
前記逆可逆演算手段は、前記復号結合情報から前記第2

付加情報を削除して復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項7】 前記可逆演算手段は、前記平文及び前記第1付加情報に、排他的論理和を施して、結合情報を生成し、  
前記逆可逆演算手段は、前記復号結合情報及び前記第2付加情報に、排他的論理和を施して、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項8】 前記可逆演算手段は、前記平文と前記第1付加情報とに加算を施して、結合情報を生成し、  
前記逆可逆演算手段は、前記復号結合情報から前記第2付加情報を減じて、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項9】 前記可逆演算手段は、前記平文及び前記第1付加情報に乗算を施して、結合情報を生成し、  
前記逆可逆演算手段は、前記復号結合情報及び前記第2付加情報に逆乗算を施して、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項10】 前記可逆演算手段は、前記第1付加情報に基づいて、前記平文のビット表現を置換して、結合情報を生成し、  
前記逆可逆演算手段は、前記第2付加情報に基づいて、前記復号結合情報のビット表現を逆置換して、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項11】 前記可逆演算手段は、前記第1付加情報に対応する変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記平文を変換して、結合情報を生成し、  
前記逆可逆演算手段は、前記第2付加情報に対応し、前記変換テーブルと同一の変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記復号結合情報を逆変換して、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項12】 前記送信装置は、平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成し、その後再度、前記送信装置は、前記平文と同一の平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成する場合において、  
前記第1生成手段は、第1付加情報と異なる第3付加情報を生成し、  
前記可逆演算手段は、前記平文及び前記第3付加情報に可逆演算を施して、結合情報を生成し、  
前記暗号手段は、前記結合情報に暗号アルゴリズムを施して暗号文を生成し、  
前記送信手段は、前記暗号文を送信し、  
前記受信手段は、前記暗号文を受信し、  
前記第2生成手段は、前記第3付加情報と同一の第4付

50 前記第2生成手段は、前記第3付加情報と同一の第4付

加情報を生成し、

前記復号手段は、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成し、

前記逆可逆演算手段は、前記復号結合情報及び第4付加情報に前記可逆演算の逆演算を施して、復号文を生成することを特徴とする請求項1に記載の暗号通信システム。

【請求項13】 前記送信装置は、前記平文に代えて、生成された前記結合情報に、前記一方向性関数を施して前記第1関数値を生成し、

前記受信装置は、前記復号文に代えて、生成された前記復号結合情報に、前記一方向性関数を施して前記第2関数値を生成し、前記第1関数値と前記第2関数値とが一致するか否かを判断することを特徴とする請求項1に記載の暗号通信システム。

【請求項14】 前記送信装置は、さらに、前記可逆変換と異なる別の可逆変換を前記平文に施して、別の結合情報を生成し、

前記送信装置は、前記平文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第1関数値を生成し、

前記受信装置は、さらに、生成された前記復号文に、前記別の可逆変換を施して、別の結合情報を生成し、

前記受信装置は、前記復号文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第2関数値を生成し、前記第1関数値と前記第2関数値とが一致するか否かを判断することを特徴とする請求項1に記載の暗号通信システム。

【請求項15】 平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信方法であって、

前記送信ステップは、前記送信装置で用いられ、前記受信ステップは、前記受信装置で用いられ、

送信ステップは、

第1付加情報を生成する第1生成ステップと、

前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算ステップと、

前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、

前記暗号文を送信する送信ステップとを含み、

受信ステップは、

前記暗号文を受信する受信ステップと、

前記第1付加情報と同一の第2付加情報を生成する第2生成ステップと、

前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施し

て復号結合情報を生成する復号ステップと、

前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする暗号通信方法。

【請求項16】 平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信プログラムであって、

前記送信ステップは、前記送信装置で用いられ、前記受信ステップは、前記受信装置で用いられ、

送信ステップは、

第1付加情報を生成する第1生成ステップと、

前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算ステップと、

前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、

前記暗号文を送信する送信ステップとを含み、

受信ステップは、

前記暗号文を受信する受信ステップと、

前記第1付加情報と同一の第2付加情報を生成する第2生成ステップと、

前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号ステップと、

前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする暗号通信プログラム。

【請求項17】 平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記送信ステップは、前記送信装置で用いられ、前記受

信ステップは、前記受信装置で用いられ、  
送信ステップは、  
第1付加情報を生成する第1生成ステップと、  
前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算ステップと、  
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、  
前記暗号文を送信する送信ステップとを含み、  
受信ステップは、  
前記暗号文を受信する受信ステップと、  
前記第1付加情報と同一の第2付加情報を生成する第2生成ステップと、  
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号ステップと、  
前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする記録媒体。

【請求項18】 平文を暗号化して暗号文を得、前記平文に一方方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置であって、  
第1付加情報を生成する第1生成手段と、  
前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、  
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、  
前記暗号文を送信する送信手段とを備えることを特徴とする送信装置。

【請求項19】 平文を暗号化して暗号文を得、前記平文に一方方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置から前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置であって、

請求項18に記載の送信装置から前記暗号文を受信する受信手段と、

前記第1付加情報と同一の第2付加情報を生成する第2生成手段と、

前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、

前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを備えることを特徴とする受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報セキュリティ技術としての暗号技術に関し、特に、復号時の誤り検出

技術に関するものである。

【0002】

【従来の技術】 近年、コンピュータ技術及び通信技術に基づくデータ通信の普及に伴い、特定の通信相手以外に通信内容を漏らすことなくデータ通信を行う暗号通信方式が広く用いられるようになってきており、暗号通信方式を実現するために、暗号方式が用いられる。

【0003】 暗号方式の中には、正規の暗号鍵を用いて平文に暗号アルゴリズムを施して暗号文を生成し、正規の復号鍵を用いて生成した前記暗号文に復号アルゴリズムを施して復号文を生成する場合に、平文と復号文とが異なる可能性がある暗号方式がある。以降、正規の復号鍵を用いて復号しても、復号文が平文と異なることを、「復号誤り」と記述し、復号誤りが生じる可能性がある暗号方式を、「復号誤りが発生し得る暗号方式」と記述する。

【0004】 上記復号誤りが発生し得る暗号方式の一例として、NTRU暗号方式がある。NTRU暗号方式は、簡単に説明すると、暗号鍵を用いて、乱数をパラメータとして用いて、平文を暗号化して暗号文を生成し、復号鍵を用いて、暗号文を復号して復号文を生成する。この方式は、乱数をパラメータとして用いて暗号化するので、平文が同じでも暗号文が異なる可能性がある。

【0005】 なお、NTRU暗号方式については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998. に詳しく述べられている。NTRU暗号方式を用いる暗号通信方式では、復号文が平文と異なる可能性があるので、意図した情報を確実に伝えることができないという問題がある。

【0006】 (従来例1) 上記の問題を解決するために、以下に示すようなNTRU暗号方式を用いる暗号通信システムが提案されている。前記暗号通信システムは、暗号装置及び復号装置から構成されている。暗号装置及び復号装置は、通信路で接続されている。暗号装置は、 $n$ 個の乱数 $r_1, r_2, \dots, r_n$ を生成し、予め記憶している暗号鍵 $K_p$ を用いて、乱数 $r_1, r_2, \dots, r_n$ をパラメータとして用いて、平文 $m$ を暗号化し、 $n$ 個の暗号文 $c_1, c_2, \dots, c_n$ を生成する。

【0007】

$$c_1 = E(m, K_p, r_1)$$

$$c_2 = E(m, K_p, r_2)$$

...

$$c_n = E(m, K_p, r_n)$$

ここで、 $C = E(M, K, R)$ は、暗号鍵 $K$ を用いて、乱数 $R$ をパラメータとして用いて、平文 $M$ を暗号化し、暗号文 $C$ を生成することを示す。

【0008】 次に、暗号装置は、生成した暗号文 $c$

$c_1, c_2, \dots, c_n$  を通信路を介して復号装置へ送信する。復号装置は、通信路を介して、 $n$  個の暗号文  $c_1, c_2, \dots, c_n$  を受信し、予め記憶している復号鍵  $Ks$  を用いて、受信した暗号文  $c_1, c_2, \dots, c_n$  を復号し、復号文  $m'_1, m'_2, \dots, m'_n$  を得る。

【0009】

$m'_1 = D(c_1, Ks)$

$m'_2 = D(c_2, Ks)$

...

$m'_n = D(c_n, Ks)$

次に、復号装置は、上記のようにして得られた復号文  $m'_1, m'_2, \dots, m'_n$  が一つでも異なっていたら復号誤りが発生したとみなす。

【0010】この暗号通信システムによると、復号誤りの発生が検出できるものの、通信量が増え、非効率的である。また、異なる乱数をパラメータとして用いて、同じ平文を暗号化した複数の暗号文を送信するので、暗号方式の安全性が低下する恐れもある。

$c_1 = E(m, Kp, r_1)$

$c_2 = E(m, Kp, r_2)$

...

$c_n = E(m, Kp, r_n)$

の  $n$  個の関係式から平文  $m$  や乱数  $r[1], r[2], \dots, r[n]$  に関する情報が第三者に漏れる恐れがあるからである。このことを利用した暗号攻撃法を、Multiple Transmission Attack と言う。

【0011】具体的には、復号誤りの発生し得る暗号方式の1つである NTRU 暗号方式を用いて、上記復号誤り検出を行うと安全性が低下することが知られている。この攻撃法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998. に詳しく述べられている。

【0012】以上説明したように、従来例1においては、復号誤りを検出しようとする、通信量が増大し、しかも安全性が低下する恐れもあるという問題点がある。

(従来例2) また、特開 2000-216773 号公報によると、暗号化された情報の受信側で、復号化した情報が正しいものであるかを判定することができる暗号化情報の正当性を判断する方法及び装置を提供することを目的として、以下のような技術が開示されている。

【0013】情報の発信側では、所定のハッシュ値生成アルゴリズムにより、平文から第1のハッシュ値を算出し、前記第1のハッシュ値と、暗号アルゴリズムを用いて平文を暗号化して得た暗号文とを送信する。情報の受信側では、前記暗号文と、前記第1のハッシュ値とを受信し、前記暗号文を復号して復号文を生成し、前記第1

のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより前記復号文から第2のハッシュ値を算出し、受信した前記第1のハッシュ値と算出した前記第2のハッシュ値とを比較し、前記第1のハッシュ値と前記第2のハッシュ値とが一致する場合に、前記復号文が正当であると判断する。

【0014】

【発明が解決しようとする課題】しかしながら、上記の従来技術を適用する場合であっても、第三者による攻撃を完全に避けることは困難であり、従来技術よりもさらに安全性の高い暗号通信システムが要望されている。本発明は、上記の要望に対応するために、さらに安全性の高い暗号通信システム、送信装置、受信装置、暗号通信方法、プログラム及びプログラムを記録している記録媒体を提供することを目的とする。

【0015】

【課題を解決するための手段】上記目的を達成するために、本発明は、平文を暗号化して暗号文を得、前記平文に一方方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、送信装置は、第1付加情報を生成する第1生成手段と、前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、前記暗号文を送信する送信手段とを含み、受信装置は、前記暗号文を受信する受信手段と、前記第1付加情報と同一の第2付加情報を生成する第2生成手段と、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含むことを特徴とする。

【0016】ここで、前記第1生成手段及び前記第2生成手段は、同期して、それぞれ同一内容の第1付加情報及び第2付加情報を生成するように構成してもよい。ここで、前記第1生成手段は、生成した前記第1付加情報を送信し、前記第2生成手段は、前記第1付加情報を受信し、受信した前記第1付加情報を第2付加情報とるように構成してもよい。

【0017】ここで、前記第1生成手段は、生成した前記第1付加情報に暗号アルゴリズムを施して、暗号化付加情報を生成して送信し、前記第2生成手段は、前記暗号化付加情報を受信し、受信した暗号化付加情報に前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して、付加情報を生成し、生成した付加情報を第2付加

情報とするように構成してもよい。

【0018】ここで、前記第1生成手段は、乱数を生成し、生成した乱数を前記第1付加情報とするように構成してもよい。ここで、前記可逆演算手段は、前記平文及び前記第1付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第2付加情報を削除して復号文を生成するように構成してもよい。

【0019】ここで、前記可逆演算手段は、前記平文及び前記第1付加情報に、排他的論理和を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び前記第2付加情報に、排他的論理和を施して、復号文を生成するように構成してもよい。ここで、前記可逆演算手段は、前記平文と前記第1付加情報とに加算を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第2付加情報を減じて、復号文を生成するように構成してもよい。

【0020】ここで、前記可逆演算手段は、前記平文及び前記第1付加情報に乗算を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び前記第2付加情報に逆乗算を施して、復号文を生成するように構成してもよい。ここで、前記可逆演算手段は、前記第1付加情報に基づいて、前記平文のビット表現を置換して、結合情報を生成し、前記逆可逆演算手段は、前記第2付加情報に基づいて、前記復号結合情報のビット表現を逆置換して、復号文を生成するように構成してもよい。

【0021】ここで、前記可逆演算手段は、前記第1付加情報に対応する変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記平文を変換して、結合情報を生成し、前記逆可逆演算手段は、前記第2付加情報に対応し、前記変換テーブルと同一の変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記復号結合情報を逆変換して、復号文を生成するように構成してもよい。

【0022】ここで、前記送信装置は、平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成し、その後再度、前記送信装置は、前記平文と同一の平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成する場合において、前記第1生成手段は、第1付加情報と異なる第3付加情報を生成し、前記可逆演算手段は、前記平文及び前記第3付加情報に可逆演算を施して、結合情報を生成し、前記暗号手段は、前記結合情報に暗号アルゴリズムを施して暗号文を生成し、前記送信手段は、前記暗号文を送信し、前記受信手段は、前記暗号文を受信し、前記第2生成手段は、前記第3付加情報と同一の第4付加情報を生成し、前記復号手段は、前記暗号文に、前記暗号アルゴリズムの逆変換であ

る復号アルゴリズムを施して復号結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び第4付加情報に前記可逆演算の逆演算を施して、復号文を生成するように構成してもよい。

【0023】ここで、前記送信装置は、前記平文に代えて、生成された前記結合情報に、前記一方向性関数を施して前記第1関数値を生成し、前記受信装置は、前記復号文に代えて、生成された前記復号結合情報に、前記一方向性関数を施して前記第2関数値を生成し、前記第1関数値と前記第2関数値とが一致するか否かを判断するように構成してもよい。

【0024】ここで、前記送信装置は、さらに、前記可逆変換と異なる別の可逆変換を前記平文に施して、別の結合情報を生成し、前記送信装置は、前記平文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第1関数値を生成し、前記受信装置は、さらに、生成された前記復号文に、前記別の可逆変換を施して、別の結合情報を生成し、前記受信装置は、前記復号文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第2関数値を生成し、前記第1関数値と前記第2関数値とが一致するか否かを判断するように構成してもよい。

【0025】

【発明の実施の形態】 1. 暗号通信システム 1

本発明に係る1個の実施の形態としての暗号通信システム1について説明する。

1. 1 暗号通信システム1の構成

暗号通信システム1は、復号誤りが発生し得る暗号通信方式における復号誤り検出が可能であるシステムであり、図1に示すように、送信装置10と受信装置20とから構成され、送信装置10と受信装置20とは、インターネット30を介して接続されている。

【0026】暗号通信システム1は、復号誤りが発生し得る暗号方式の一例として、NTRU暗号方式を用いる。NTRU暗号、及びNTRU暗号方式の暗号鍵、及び復号鍵の生成方法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem", Lecture Notes in Computer Science, 1423, pp.267-288, Springer-Verlag, 1998.に詳しく述べられている。

【0027】送信装置10は、予め記憶している平文にNTRU暗号方式による暗号アルゴリズムを施して暗号文を生成し、生成した暗号文を受信装置20へ送信する。受信装置20は、暗号文を受信し、受信した暗号文にNTRU暗号方式による復号アルゴリズムを施して復号文を生成する。

1. 2 送信装置10の構成

送信装置10は、平文記憶部101、付加情報生成部102、情報付加部103、一方向性関数部104、暗号化部105及び送信部106から構成される。送信装置



10は、具体的には、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスクプレイユニット、キーボード、マウス、通信部などから構成されるコンピュータシステムである。前記RAM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

#### 【0028】(1) 平文記憶部101

平文記憶部101は、予め平文 $m$ を記憶している。平文 $m$ は、固定長の情報から構成される。

#### (2) 付加情報生成部102

付加情報生成部102は、予め決められたビット数 $rLen$ の長さの乱数である付加情報 $Ra$ を生成し、生成した付加情報 $Ra$ を情報付加部103へ出力する。

#### 【0029】(3) 情報付加部103

情報付加部103は、平文記憶部101から平文 $m$ を読み出し、付加情報生成部102から付加情報 $Ra$ を受け取る。次に、情報付加部103は、読み出した平文 $m$ と受け取った付加情報 $Ra$ とを結合して、平文 $m$ に付加情報 $Ra$ をビット結合した結果である結合情報 $F(m, Ra) = m || Ra$ を算出する。

【0030】ここで、演算子「 $||$ 」は、ビット結合を示す。ビット結合という操作は、2つの値をビット列で表現し、それらを結合したものを1つの値とする操作である。例えば、 $m=10$ 、 $rLen=5$ 、 $Ra=7$ とすると、平文 $m$ のビット列表現は「1010」、長さ $rLen$ の付加情報 $Ra$ のビット列表現は「00111」となるので、ビット結合した結果は、「101000111」となり、これは十進数で327である。

【0031】次に、情報付加部103は、生成した結合情報 $F(m, Ra)$ を暗号化部105へ出力する。

#### (4) 一方向性関数部104

一方向性関数部104は、予め一方向性関数としてハッシュ関数 $h$ を有している。

【0032】ここで、一方向性関数とは、入力された値から関数値を計算することは容易であるが、関数値から関数に入力された元の値を求めることが困難な関数のことである。また、ここで用いるハッシュ関数 $h$ は、関数の値 $h(m)$ から平文 $m$ の値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。

なお、一方向性関数、ハッシュ関数、ハッシュ関数の安全性、及びハッシュ関数の衝突困難性については、「現代暗号」(岡本龍明、山本博資著、シリーズ/情報科学の数学、産業図書、1997、56ページ及び189～195ページ)に詳しく述べられている。

【0033】一方向性関数部104は、平文記憶部101から平文 $m$ を読み出し、読み出した平文 $m$ にハッシュ関数 $h$ による演算を施して関数値 $h(m)$ を生成し、生成した関数値 $h(m)$ を送信部106へ出力する。

#### (5) 暗号化部105

暗号化部105は、乱数生成部1051、暗号鍵記憶部1052及び暗号化関数部1053から構成されている。

【0034】(暗号鍵記憶部1052) 暗号鍵記憶部1052は、予め暗号鍵 $Kp$ を記憶している。

(乱数生成部1051) 乱数生成部1051は、一例として、C言語のライブラリ関数である $rand()$ を用いて乱数 $r$ を生成し、生成した乱数 $r$ を暗号化関数部1053へ出力する。

【0035】(暗号化関数部1053) 暗号化関数部1053は、予めNTRU暗号方式の暗号アルゴリズムを有している。暗号化関数部1053は、情報付加部103から結合情報 $F(m, Ra)$ を受け取り、乱数生成部1051から乱数 $r$ を受け取り、暗号鍵記憶部1052から暗号鍵 $Kp$ を読み出す。

【0036】次に、暗号化関数部1053は、受け取った乱数 $r$ を使用して、読み出した暗号鍵 $Kp$ を用いて、受け取った結合情報 $F(m, Ra)$ に前記暗号アルゴリズムを施して、暗号化結合情報 $E(F(m, Ra), Kp, r)$ を生成し、生成した暗号化結合情報 $E(F(m, Ra), Kp, r)$ を送信部106へ出力する。

#### (6) 送信部106

送信部106は、暗号化結合情報 $E(F(m, Ra), Kp, r)$ と、関数値 $h(m)$ とを受け取り、受け取った暗号化結合情報 $E(F(m, Ra), Kp, r)$ と、関数値 $h(m)$ とをインターネット30を介して受信装置20へ送信する。

#### 【0037】1.3 受信装置20の構成

受信装置20は、受信部201、復号化部202、情報除去部203、一方向性関数部204、比較部205、復号文記憶部206及び比較結果記憶部207から構成される。受信装置20は、具体的には、送信装置10と同様のコンピュータシステムである。

#### 【0038】(1) 受信部201

受信部201は、送信装置10からインターネット30を介して、暗号化結合情報 $E(F(m, Ra), Kp, r)$ と関数値 $h(m)$ とを受信し、受信した暗号化結合情報 $E(F(m, Ra), Kp, r)$ を復号化部202へ出力し、受信した関数値 $h(m)$ を比較部205へ出力する。

#### 【0039】(2) 復号化部202

復号化部202は、復号鍵記憶部2021及び復号化関数部2022から構成される。

(復号鍵記憶部2021) 復号鍵記憶部2021は、予め復号鍵 $Ks$ を記憶している。

【0040】(復号化関数部2022) 復号化関数部2022は、暗号化関数部1053が有する暗号アルゴリズムの逆変換である復号アルゴリズムを予め有している。復号化関数部2022は、受信部201から暗号化

結合情報E ( $F(m, Ra)$ 、 $Kp$ 、 $r$ )を受け取り、復号鍵記憶部2021から復号鍵 $Ks$ を読み出す。

【0041】次に、復号化関数部2210は、読み出した復号鍵 $Ks$ を用いて、受け取った暗号化結合情報E ( $F(m, Ra)$ 、 $Kp$ 、 $r$ )に前記復号アルゴリズムを施して、復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )、 $Ks$ )を生成し、生成した復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )、 $Ks$ )を情報除去部2250へ出力する。

【0042】(3) 情報除去部203

情報除去部203は、予めビット数 $rLen$ を記憶している。情報除去部203は、復号化部202から復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )、 $Ks$ )を受け取り、受け取った復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )、 $Ks$ )の末尾からビット数 $rLen$ 分のビット列を除去することにより、復号結合情報から付加情報 $Ra$ を除去し、復号結合情報から付加情報 $Ra$ が除去された残りの情報を復号文 $m'$ として生成し、生成した復号文 $m'$ を一方方向性関数部204へ出力する。また、生成した復号文 $m'$ を復号文記憶部206へ書き込む。

【0043】(4) 一方方向性関数部204

一方方向性関数部204は、一方方向性関数部104が有しているハッシュ関数 $h$ と同じハッシュ関数を予め有している。一方方向性関数部204は、情報除去部203から復号文 $m'$ を受け取り、受け取った復号文 $m'$ にハッシュ関数 $h$ による演算を施して関数値 $h(m')$ を生成し、生成した関数値 $h(m')$ を比較部205へ出力する。

【0044】(5) 比較部205

比較部205は、受信部201から関数値 $h(m)$ を受け取り、一方方向性関数部204から関数値 $h(m')$ を受け取る。次に、比較部205は、関数値 $h(m)$ と関数値 $h(m')$ とを比較して、一致するか否かを判断し、一致又は不一致を示す比較結果 $j$ を生成する。具体的には、比較部205は、一致する場合には、比較結果 $j=1$ とし、一致しない場合には、比較結果 $j=0$ とする。次に、生成した比較結果 $j$ を比較結果記憶部207に書き込む。

【0045】(6) 復号文記憶部206

復号文記憶部206は、復号文を記憶するための領域を備えている。

(7) 比較結果記憶部207

比較結果記憶部207は、比較結果 $j$ を記憶するための領域を備えている。

1. 4 送信装置10の動作

送信装置10の動作について、図4～図5に示すフローチャートを用いて説明する。

【0046】付加情報生成部102は、付加情報 $Ra$ を生成し、生成した付加情報 $Ra$ を情報付加部103へ出

力する(ステップS101)。次に、情報付加部103は、平文記憶部101から平文 $m$ を読み出し(ステップS102)、付加情報生成部102から付加情報 $Ra$ を受け取り(ステップS103)、読み出した平文 $m$ と受け取った付加情報 $Ra$ とを結合して、結合情報 $F(m, Ra)$ を生成し、生成した結合情報 $F(m, Ra)$ を暗号化部105へ出力する(ステップS104)。

【0047】次に、暗号化部105は、結合情報 $F(m, Ra)$ を受け取り、受け取った結合情報 $F(m, Ra)$ に暗号アルゴリズム $E$ を施して暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を生成し(ステップS105)、生成した暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を送信部106へ出力する(ステップS106)。

【0048】次に、一方方向性関数部104は、平文記憶部101から平文 $m$ を読み出し(ステップS107)、読み出した平文 $m$ にハッシュ関数 $h$ による演算を施して関数値 $h(m)$ を生成し(ステップS108)、生成した関数値 $h(m)$ を送信部106へ出力する(ステップS109)。送信部106は、暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )と、関数値 $h(m)$ とを受け取り、受け取った暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )と、関数値 $h(m)$ とをインターネット30を介して受信装置20へ送信する(ステップS110)。

【0049】1. 5 受信装置20の動作

受信装置20の動作について、図6に示すフローチャートを用いて説明する。受信部201は、送信装置10からインターネット30を介して、暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )と関数値 $h(m)$ とを受信し(ステップS151)、受信した暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を復号化部202へ出力し、受信した関数値 $h(m)$ を比較部205へ出力する(ステップS152)。

【0050】復号化部202は、暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を受け取り、受け取った暗号化結合情報 $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )に復号アルゴリズム $D$ を施して復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を生成し(ステップS153)、復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を情報除去部203へ出力する(ステップS154)。

【0051】情報除去部203は、復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )を受け取り、受け取った復号結合情報D ( $E(F(m, Ra)$ 、 $Kp$ 、 $r$ )から付加情報 $Ra$ を除去して、復号文 $m'$ を生成し(ステップS155)、生成した復号文 $m'$ を一方方向性関数部204へ出力し、生成した復号文 $m'$ を復号文記憶部206へ書き込む(ステップS156)。

【0052】一方方向性関数部204は、復号文 $m'$ を受け取り、受け取った復号文 $m'$ にハッシュ関数 $h$ による

演算を施して関数値  $h(m')$  を生成し、生成した関数値  $h(m')$  を比較部 205 へ出力する（ステップ S157）。比較部 205 は、関数値  $h(m)$  と関数値  $h(m')$  とを受け取り、受け取った関数値  $h(m)$  と関数値  $h(m')$  とを比較して、一致するか否かを判断し、一致又は不一致を示す比較結果  $j$  を生成し、生成した比較結果  $j$  を比較結果記憶部 207 に書き込む（ステップ S158）。

【0053】 1.6 実施の形態における動作検証と従来例との比較

以下に、本実施の形態における復号誤りの検出について説明する。また、従来技術による方法との比較を行う。復号誤りが発生していない場合において、受信装置 20 の比較部 205 が出力する比較結果  $j$  は常に 1 である。

【0054】 また、復号誤りが発生している場合に、受信装置 20 の比較部 205 が出力する比較結果  $j$  が 1 となる確率は、即ち、受信装置 20 の一方向性関数部 204 によって生成された  $h(m')$  が、送信装置 10 の一方向性関数部 104 によって生成された  $h(m)$  と偶然等しくなる確率は、次のようになる。一方向性関数部 104 及び一方向性関数部 204 において、 $k$  ビットのハッシュ値を出力するハッシュ関数を用いる場合、ハッシュ関数により出力される  $k$  ビットのハッシュ値は  $2^k$  通り存在するので、前記確率は、 $2^{-k}$  となる。

【0055】 従って、実際に復号誤りが発生したとき、受信装置 20 により生成される比較結果  $j$  を調べることによって、 $1 - 2^{-k}$  の確率で、復号誤りが発生したことを確認することができる。例えば、一方向性関数部 104 及び一方向性関数部 204 で用いられるハッシュ関数を SHA-1 とするとき、SHA-1 は 160 ビットの出力を持つので、この確率は  $1 - 2^{-160}$  となり、ほぼ復号誤りの発生を検出することができるといえる。

【0056】 また、インターネット 30 を介して通信される通信量は、暗号化部 105 が出力する暗号文のビット長と一方向性関数部 104 が出力するハッシュ値のビット長を合わせた量である。一般にハッシュ関数の出力ビット長は入力データの出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の 2 倍を超えることはない。

【0057】 例えば、ハッシュ関数に SHA-1 を使う場合、NTRU 暗号方式を含む暗号方式では暗号文長が 160 ビット以上のものが使われることが多いので、このことは成り立つ。従来例 1 のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例 1 のデータ暗号化システムに比べて、この本実施の形態では通信量が少なくなり、通信効率が向上する。

【0058】 さらに、安全性については、ハッシュ関数は、出力の値から入力の値を得ることは困難であり、また、従来例 1 のように同じ平文を複数回送信することは

ないので、十分な安全性が確保できる。加えて、復号誤り検出の後に、再送要求を行い、同じデータを再度送信させるプロトコルを採用する場合においても、平文に乱数が付加されて暗号化されているので、従来例 1 に示すような Multiple Transmission Attack に対して、本実施の形態では、従来例 1 のデータ暗号化システムよりも耐性を持っている。

【0059】 また、従来技術によると、平文をそのまま暗号化して送信しているので、受信者からの再送要求に応じて、送信者が同じ平文を暗号化して生成した暗号文を再送する場合、通信路を傍受する第三者に平文を解読される可能性が高くなる。つまり、第三者が傍受した複数の暗号文から平文が解読される恐れがある。この攻撃方法は、Multiple Transmission Attack と呼ばれる。

【0060】 これに対し、本実施の形態によると、通信毎に付加情報  $Ra$  を異なる内容に設定できるので、受信者からの再送要求に応じて、送信者が暗号文を再送する場合に、平文自体は同じであっても、 $m || Ra$  の値は、通信の都度異なり、第三者は、Multiple Transmission Attack を適用できず、平文が不正に解読される可能性が低くなる。

【0061】 また、通信路の伝送品質が低いために、伝送される暗号文にビット落ちや、ビット化けが発生した場合であっても、上記と同様にして、元の平文と復号文との違いが検出できる。

## 2. 変形例

暗号通信システム 1 の変形例について、説明する。

### 【0062】 2.1 付加情報の変形例

暗号通信システム 1 において、付加情報生成部 102 は、乱数である付加情報  $Ra$  を生成するとしているが、タイムスタンプ情報又はカウンタ情報を生成するとしてもよい。付加情報生成部 102 が生成する付加情報は、用いる度に異なる値となるものであれば、どのような情報であってもよい。

【0063】 タイムスタンプ情報は、付加情報生成部 102 が付加情報を生成する現在時刻であり、具体的には、年、月、日、時、分、秒、ミリ秒から構成される固定長の情報である。また、カウンタ情報は、固定桁数の数値情報であり、利用される都度、1 の値が加算される情報である。

### 【0064】 2.2 結合情報 $F(m, Ra)$ 算出の変形例

暗号通信システム 1 において、情報付加部 103 は、平文  $m$  と付加情報  $Ra$  とを結合して、結合情報  $F(m, Ra) = m || Ra$  を算出するとしているが、算出方法は、付加情報に基づく  $m$  の可逆変換であれば、その他の方法であってもよい。

【0065】 前記算出方法を含めて、その他の算出方法を以下に示す。情報除去部 203 において、結合情報が

ら付加情報を除去して、平文のみを抽出するためには、算出方法に対して、それぞれ逆の演算を行う。

(1) 算出方法1

結合情報  $F(m, Ra) = m \parallel Ra$

ここで、「 $\parallel$ 」は、ビット結合を示す。(この算出方法は、上記の実施の形態において示す算出方法である。)

なお、結合情報  $F(m, Ra) = Ra \parallel m$  としてもよい。

【0066】また、平文  $m$  を4ビットずつの複数個の部分平文情報に分割する。また、付加情報を4ビットずつの複数個の部分付加情報に分割する。次に、部分平文情報と部分付加情報とを交互に結合することにより、結合情報を得るとしてもよい。一般に、平文  $m$  の長さ  $>$  付加情報の長さであるので、結合情報の後部は、部分平文情報のみが結合される。

【0067】(2) 算出方法2

結合情報  $F(m, Ra) = m (+) Ra$

ここで、「 $(+)$ 」は、排他的論理和を示す。また、逆の演算は、次の通りである。

復号文  $m' = \text{結合情報 } F (+) Ra$

(3) 算出方法3

結合情報  $F(m, Ra) = m + Ra$

また、逆の演算は、次の通りである。

【0068】復号文  $m' = \text{結合情報 } F - Ra$

(4) 算出方法4

結合情報  $F(m, Ra) = m \times Ra \bmod p$

ここで、 $p$  は、 $m$  より大きい素数である。また、逆の演算は、次の通りである。

【0069】

復号文  $m' = \text{結合情報 } F / Ra \bmod p$

(5) 算出方法5

結合情報  $F(m, Ra) = \text{BitPerm}[Ra](m)$

ここで、 $\text{BitPerm}[Ra](m)$  は、 $Ra$  に基づいて、 $m$  のビット表現を置換する演算を示す。

【0070】具体的には、以下のような演算である。

(5-1) 算出方法5-1

$m$  を、 $Ra$  ビットだけ、ビットローテートさせる。

(例) 置換前の  $m = \text{「1111000011110000」}$  をとし、 $Ra = 3$  (10進数表現) とすると、置換後の  $m = \text{「1000011110000111」}$  となる。

【0071】ここで、逆方向のビットローテートとしてもよい。また、逆の演算は、次の通りである。結合情報  $F$  を、 $Ra$  ビットだけ、逆方向へビットローテートさせる。

(5-2) 算出方法5-2

$m$  を、計算アルゴリズムにより置換する。言い換えると、 $Ra$  を入力値とする演算をし、その演算結果に基づいて、 $m$  を、置換する。

【0072】(例)  $Ra$  を128ビット長とする。 $Ra$  にハッシュ関数を施して、16ビット長のハッシュ値を得る。次に、算出方法5-1に示すように、得られたハッシュ値だけ、 $m$  をビットローテートさせる。また、逆の演算は、次の通りである。結合情報  $F$  を、計算アルゴリズムにより置換する。言い換えると、 $Ra$  を入力値とする演算をし、その演算結果に基づいて、結合情報  $F$  を、置換して、復号文  $m'$  を得る。

【0073】(例)  $Ra$  を128ビット長とする。 $Ra$  にハッシュ関数を施して、16ビット長のハッシュ値を得る。次に、算出方法5-1に示すように、得られたハッシュ値だけ、結合情報  $F$  を逆方向にビットローテートさせる。

(5-3) 算出方法5-3

$m$  を4ビットずつに区切って複数の部分情報を生成する。次に、部分情報毎に、 $Ra$  に対応する入出力4ビットの置換テーブルを用いて、置換する。

【0074】ここで、置換テーブルは、4ビットの変換前ビット列と対応する4ビットの変換後ビット列とからなる組を、16個含む。ある値(例えば、「1」)の  $Ra$  に対応する置換テーブルにおいて、16個の変換前ビット列は、「0000」、「0001」、「0010」、・・・、「1110」及び「1111」である。これらに対応する16個の変換後ビット列は、「1111」、「1110」、「1101」、・・・、「0001」及び「0000」である。

【0075】また、別の値(例えば、「2」)の  $Ra$  に対応する置換テーブルにおいて、16個の変換前ビット列に対応する16個の変換後ビット列は、「1111」、「1110」、「1101」、・・・、「0000」及び「0001」である。このように、 $Ra$  の値に対応して複数種類の置換テーブルが存在する。また、逆の演算は、次の通りである。

【0076】結合情報  $F$  を4ビットずつに区切って複数の部分結合情報を生成する。次に、部分結合情報毎に、 $Ra$  に対応する入出力4ビットの置換テーブルを用いて、上記の逆方向の置換を行う。

(6) 算出方法6

結合情報  $F(m, Ra) = \text{Tab}[Ra](m)$

ここで、 $\text{Tab}[Ra](m)$  は、 $m$  を変換テーブル  $\text{Tab}$  に従って変換することを示す。

【0077】例えば、 $m$  が8ビット長の場合、 $Ra$  の値毎に、例えば、図7に示すような変換テーブル  $\text{Tab}$  を記憶しておき、変換テーブル  $\text{Tab}$  に従って、 $m$  の値を変換する。変換テーブル  $\text{Tab}$  は、8ビットの値と8ビットの値を対応付けた組を256個含む。例えば、 $m = 1$  の場合、図7に示す変換テーブル  $\text{Tab}$  に基づいて、平文  $m$  は、39に変換される。

【0078】また、逆の演算は、次の通りである。結合情報  $F$  を変換テーブル  $\text{Tab}$  に従って、上記と逆方向に

変換する。

## 2. 3 付加情報を共有するための暗号通信システムの変形例

送信装置10と受信装置20とにおいて、付加情報を共有するための暗号通信システムの変形例について、以下に説明する。

### 【0079】(1) 第1の変形例

暗号通信システム1の第1の変形例としての暗号通信システム1bについて説明する。

(暗号通信システム1bの構成) 暗号通信システム1bは、図8に示すように、送信装置10b及び受信装置20bから構成される。

【0080】送信装置10b及び受信装置20bは、それぞれ、暗号通信システム1を構成する送信装置10及び受信装置20と、同様の構成を有している。以下において、送信装置10及び受信装置20との相違点を中心として説明する。送信装置10bは、さらに、同期部107を備えている。また、送信装置10bは、付加情報生成部102に代えて、付加情報生成部102bを備えている。また、受信装置20bは、さらに、同期部208及び付加情報生成部209を備えている。同期部107と同期部208とは、専用回線40bを介して接続されている。

【0081】同期部107は、乱数XRを生成し、生成した乱数XRを専用回線40bを介して同期部208へ出力する。また、生成した乱数XRを付加情報生成部102へ出力する。付加情報生成部102は、同期部107から乱数XRを受け取り、受け取った乱数XRを用いて、付加情報Raを生成し、生成した付加情報Raを情報付加部103へ出力する。ここで、乱数XRを用いて付加情報Raを生成する一例として、付加情報生成部102は、乱数XRをそのまま付加情報Raとする。

【0082】同期部208は、専用回線40bを介して、付加情報XRを受け取り、受け取った付加情報XRを付加情報生成部209へ出力する。付加情報生成部209は、同期部208から乱数XRを受け取り、受け取った乱数XRを用いて、付加情報Raを生成し、生成した付加情報Raを情報除去部203へ出力する。ここで、乱数XRを用いて付加情報Raを生成する一例として、付加情報生成部209は、乱数XRをそのまま付加情報Raとする。

【0083】(暗号通信システム1bの動作) 暗号通信システム1bの動作について、図9に示すフローチャートを用いて説明する。なお、暗号通信システム1bの動作は、暗号通信システム1の動作と同様であるので、ここでは相違点を中心として説明する。

【0084】同期部107は、乱数XRを生成し(ステップS201)、生成した乱数XRを専用回線40bを介して同期部208へ出力する(ステップS202)。また、生成した乱数XRを付加情報生成部102へ出力

する(ステップS203)。付加情報生成部102は、同期部107から乱数XRを受け取り、受け取った乱数XRを用いて、付加情報Raを生成し、生成した付加情報Raを情報付加部103へ出力する(ステップS203)。

【0085】同期部208は、専用回線40bを介して、乱数XRを受け取り、受け取った乱数XRを付加情報生成部209へ出力する(ステップS202)。付加情報生成部209は、同期部208から乱数XRを受け取り、受け取った乱数XRを用いて、付加情報Raを生成し(ステップS204)、生成した付加情報Raを情報除去部203へ出力する(ステップS205)。情報除去部203は、付加情報Raを受け取り(ステップS205)、受け取った付加情報Raを用いて、復号結合情報から復号文m'を生成する(ステップS206)。

### 【0086】(2) 第2の変形例

暗号通信システム1の第2の変形例としての暗号通信システム1cについて説明する。

(暗号通信システム1cの構成) 暗号通信システム1cは、図10に示すように、送信装置10c及び受信装置20cから構成される。

【0087】送信装置10c及び受信装置20cは、それぞれ、暗号通信システム1を構成する送信装置10及び受信装置20と、同様の構成を有している。送信装置10cは、付加情報生成部102及び送信部106に代えて、付加情報生成部102c及び送信部106cを備えている。また、受信装置20cは、情報除去部203及び受信部201に代えて、情報除去部203c及び受信部201cを備えている。

【0088】付加情報生成部102c、送信部106c、情報除去部203c及び受信部201cは、それぞれ付加情報生成部102、送信部106、情報除去部203及び受信部201と同様の構成を有している。以下において相違点を中心として説明する。付加情報生成部102cは、生成した付加情報Raを送信部106cへ出力する。

【0089】送信部106cは、付加情報生成部102cから付加情報Raを受け取り、受け取った付加情報Raをインターネット30を介して、受信装置20cへ送信する。受信部201cは、送信装置10cからインターネット30を介して、付加情報Raを受信し、受信した付加情報Raを情報除去部203cへ出力する。

【0090】情報除去部203cは、受信部201cから付加情報Raを受け取り、受け取った付加情報Raを用いて、復号結合情報から復号文m'を生成する。

(暗号通信システム1cの動作) 暗号通信システム1cの動作について、図11に示すフローチャートを用いて説明する。

【0091】なお、暗号通信システム1cの動作は、暗号通信システム1の動作と同様であるので、ここでは相

遠点を中心として説明する。付加情報生成部102cは、付加情報Raを生成し、生成した付加情報Raを送信部106cへ出力する(ステップS221)。送信部106cは、付加情報生成部102cから付加情報Raを受け取り、受け取った付加情報Raをインターネット30を介して、受信装置20cへ送信する(ステップS222)。

【0092】受信部201cは、送信装置10cからインターネット30を介して、付加情報Raを受信し、受信した付加情報Raを情報除去部203cへ出力する(ステップS222)。情報除去部203cは、受信部201cから付加情報Raを受け取り(ステップS223)、受け取った付加情報Raを用いて、復号結合情報から復号文m'を生成する(ステップS224)。

【0093】(3)第3の変形例

暗号通信システム1の第3の変形例としての暗号通信システム1dについて説明する。

(暗号通信システム1dの構成)暗号通信システム1dは、図12に示すように、送信装置10d及び受信装置20dから構成される。

【0094】送信装置10d及び受信装置20dは、それぞれ、暗号通信システム1を構成する送信装置10及び受信装置20と、同様の構成を有している。送信装置10dは、付加情報生成部102、暗号化部105及び送信部106に代えて、付加情報生成部102d、暗号化部105d及び送信部106dを備えている。また、受信装置20dは、復号化部202、情報除去部203及び受信部201に代えて、復号化部202d、情報除去部203d及び受信部201dを備えている。

【0095】付加情報生成部102d、暗号化部105d、送信部106d、復号化部202d、情報除去部203d及び受信部201dは、それぞれ付加情報生成部102、暗号化部105、送信部106、復号化部202、情報除去部203及び受信部201と同様の構成を有している。以下において相違点を中心として説明する。

【0096】付加情報生成部102dは、付加情報Raを生成し、生成した付加情報Raを暗号化部105dへ出力する。暗号化部105dは、付加情報生成部102dから付加情報Raを受け取り、受け取った付加情報Raに暗号アルゴリズムを施して、暗号化付加情報E(Ra, Kp, r2)を生成する。ここで、r2は、rと同様の乱数である。次に、生成した暗号化付加情報E(Ra, Kp, r2)を送信部106dへ出力する。

【0097】送信部106dは、暗号化部105dから暗号化付加情報E(Ra, Kp, r2)を受け取り、受け取った暗号化付加情報E(Ra, Kp, r2)をインターネット30を介して、受信装置20dへ送信する。受信部201dは、受信装置20dからインターネット30を介して、暗号化付加情報E(Ra, Kp, r2)

を受信し、受信した暗号化付加情報E(Ra, Kp, r2)を復号化部202dへ出力する。

【0098】復号化部202dは、受信部201dから暗号化付加情報E(Ra, Kp, r2)を受け取り、受け取った暗号化付加情報E(Ra, Kp, r2)に復号アルゴリズムを施して、復号付加情報D(E(Ra, Kp, r2), Ks)を生成する。次に、生成した復号付加情報D(E(Ra, Kp, r2), Ks)を情報除去部203dへ出力する。

10 【0099】情報除去部203dは、復号化部202dから復号付加情報D(E(Ra, Kp, r2), Ks)を受け取り、受け取った復号付加情報D(E(Ra, Kp, r2), Ks)を用いて、復号結合情報D(E(F(m, Ra), Kp, r), Ks)から復号文m'を生成する。

(暗号通信システム1dの動作)暗号通信システム1dの動作について、図13に示すフローチャートを用いて説明する。

【0100】なお、暗号通信システム1dの動作は、暗号通信システム1の動作と同様であるので、ここでは相違点を中心として説明する。付加情報生成部102dは、付加情報Raを生成し、生成した付加情報Raを暗号化部105dへ出力する(ステップS241)。暗号化部105dは、付加情報生成部102dから付加情報Raを受け取り、受け取った付加情報Raに暗号アルゴリズムを施して、暗号化付加情報E(Ra, Kp, r2)を生成し、生成した暗号化付加情報E(Ra, Kp, r2)を送信部106dへ出力する(ステップS242)。

30 【0101】送信部106dは、暗号化部105dから暗号化付加情報E(Ra, Kp, r2)を受け取り、受け取った暗号化付加情報E(Ra, Kp, r2)をインターネット30を介して、受信装置20dへ送信する(ステップS243)。受信部201dは、受信装置20dからインターネット30を介して、暗号化付加情報E(Ra, Kp, r2)を受信し、受信した暗号化付加情報E(Ra, Kp, r2)を復号化部202dへ出力する(ステップS243)。

40 【0102】復号化部202dは、受信部201dから暗号化付加情報E(Ra, Kp, r2)を受け取り、受け取った暗号化付加情報E(Ra, Kp, r2)に復号アルゴリズムを施して、復号付加情報D(E(Ra, Kp, r2), Ks)を生成し、生成した復号付加情報D(E(Ra, Kp, r2), Ks)を情報除去部203dへ出力する(ステップS244)。

50 【0103】情報除去部203dは、復号化部202dから復号付加情報D(E(Ra, Kp, r2), Ks)を受け取り(ステップS245)、受け取った復号付加情報D(E(Ra, Kp, r2), Ks)を用いて、復号結合情報D(E(F(m, Ra), Kp, r), K

s) から復号文  $m'$  を生成する (ステップ S246)。

#### 2. 4 変形例の実現可能な組合せ

付加情報の変形例、結合情報  $F(m, Ra)$  算出の変形例、及び付加情報を共有するための暗号通信システム変形例の、実現可能な組合せについて、図 14 に示す表を用いて説明する。

【0104】この表に示すように、付加情報の各変形例 (乱数、タイムスタンプ及びカウンタ) は、結合情報  $F(m, Ra)$  算出の変形例、及び付加情報を共有するための暗号通信システム変形例において、適用可能である。また、この表に示すように、結合情報  $F(m, Ra)$  算出の変形例のうち、 $m || Ra$  による結合情報の算出方法は、暗号通信システム 1、1b~1d において、適用可能である。

【0105】また、この表に示すように、結合情報  $F(m, Ra)$  算出の変形例のうち、 $m (+) Ra$ 、 $m + Ra$ 、 $m \times Ra \bmod p$ 、 $\text{BitPerm}[Ra]$  ( $m$ )、 $\text{Tab}[Ra]$  ( $m$ ) による結合情報の算出方法は、暗号通信システム 1b~1d において、適用可能である。

#### 3. その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのももちろんである。以下のような場合も本発明に含まれる。

【0106】(1) 暗号通信システム 1 は、次のように構成してもよい。

送信装置 10 の一方向性関数部 104 は、情報付加部 103 から結合情報  $F(m, Ra)$  を受け取り、受け取った結合情報  $F(m, Ra)$  にハッシュ関数を施して、関数値  $h(F(m, Ra))$  を生成し、生成した関数値  $h(F(m, Ra))$  を送信部 106、インターネット 30、受信部 201 を介して、比較部 205 へ送信する。

【0107】一方、受信装置 20 の一方向性関数部 204 は、復号化部 202 から復号結合情報  $D(E(F(m, Ra), Kp, r), Ks)$  を受け取り、受け取った復号結合情報  $D(E(F(m, Ra), Kp, r), Ks)$  にハッシュ関数を施して、関数値  $h(D(E(F(m, Ra), Kp, r), Ks))$  を生成し、生成した関数値  $h(D(E(F(m, Ra), Kp, r), Ks))$  を比較部 205 へ出力する。比較部 205 は、関数値  $h(F(m, Ra))$  と、関数値  $h(D(E(F(m, Ra), Kp, r), Ks))$  を比較して、一致するか否かを判断する。

【0108】このようにして、平文が正しく復号できたか否かを判断することができる。

(2) 暗号通信システム 1 は、次のように構成してもよい。

送信装置 10 の情報付加部 103 は、さらに、 $F$  とは異なる可逆変換である  $G$  を用いて、結合情報  $G(m, R$

$a)$  を生成する。ここで、 $G$  の具体例は、 $G = Ra || m$  である。次に、情報付加部 103 は、生成した結合情報  $G(m, Ra)$  を一方向性関数部 104 へ出力する。一方向性関数部 104 は、情報付加部 103 から結合情報  $G(m, Ra)$  を受け取り、受け取った結合情報  $G(m, Ra)$  にハッシュ関数を施して、関数値  $h(G(m, Ra))$  を生成し、生成した関数値  $h(G(m, Ra))$  を送信部 106、インターネット 30、受信部 201 を介して、比較部 205 へ送信する。

10 【0109】一方、受信装置 20 の情報除去部 203 は、さらに、生成した復号文  $m'$  及び乱数  $Ra$  に  $G$  を用いて、結合情報  $G(m', Ra)$  を生成して、一方向性関数部 204 へ出力する。ここで、情報除去部 203 は、上述の変形例に示すようにして、送信装置 10 との間で同じ乱数  $Ra$  を共有する。一方向性関数部 204 は、結合情報  $G(m', Ra)$  を受け取り、受け取った結合情報  $G(m', Ra)$  にハッシュ関数を施して、関数値  $h(G(m', Ra))$  を生成し、生成した関数値  $h(G(m', Ra))$  を比較部 205 へ出力する。比較部 205 は、関数値  $h(G(m, Ra))$  と関数値  $h(G(m', Ra))$  とを比較して、一致するか否かを判断する。

【0110】このようにして、平文が正しく復号できたか否かを判断することができる。

(3) 暗号アルゴリズム及び復号アルゴリズムは、上記の実施の形態に示したアルゴリズムに限定されない。他の暗号アルゴリズムを適用してもよい。例えば、DES 暗号方式、RSA 暗号方式や ElGamal 暗号方式などの一般の暗号方式が適用できる。

30 【0111】また、一方向性関数部 104 は、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。なお、DES 暗号方式、RSA 暗号方式、及び ElGamal 暗号方式については、岡本龍明、山本博資、「現代暗号」、シリーズ/情報科学の数学、産業図書、1997 に詳しく述べられている。

【0112】さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なってもよい。

40 (4) 本実施の形態では、送信装置 10 と受信装置 20 とは、インターネット 30 を介して接続されているとしているが、インターネットには限定されない。専用回線、無線通信路などにより接続されているとしてもよい。

【0113】(5) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み



取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0114】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0115】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(6) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0116】

【発明の効果】上記目的を達成するために、本発明は、平文を暗号化して暗号文を得、前記平文に一方方向性関数を施して第1関数値を得、前記暗号文と前記第1関数値とを送信する送信装置、及び前記暗号文と前記第1関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方方向性関数を施して第2関数値を得、前記第2関数値と前記第1関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、送信装置は、第1付加情報を生成する第1生成手段と、前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、前記暗号文を送信する送信手段とを含み、受信装置は、前記暗号文を受信する受信手段と、前記第1付加情報と同一の第2付加情報を生成する第2生成手段と、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含む。

【0117】この構成によると、前記送信装置は、前記平文及び前記第1付加情報に可逆演算を施して、結合情報を生成し、前記結合情報を暗号化して暗号化結合情報を生成して送信し、前記受信装置は、前記暗号化結合情報を受信して復号して復号結合情報を生成し、前記復号結合情報及び第2付加情報に前記可逆演算の逆演算を施して、復号文を生成するので、従来技術よりもさらに安

全性の高い暗号通信システムを実現できる。

【0118】ここで、前記第1生成手段及び前記第2生成手段は、同期して、それぞれ同一内容の第1付加情報及び第2付加情報を生成する。この構成によると、前記第1生成手段及び前記第2生成手段が、同期して、それぞれ同一内容の第1付加情報及び第2付加情報を生成するので、結合情報と同一内容の復号結合情報が得られると期待できる。

【0119】ここで、前記第1生成手段は、乱数を生成し、生成した乱数を前記第1付加情報とする。この構成によると、前記第1生成手段は、乱数を用いて第1付加情報を生成するので、通信毎に第1付加情報が異なり、暗号化結合情報から第1付加情報を推定することが困難となる。

【0120】ここで、前記可逆演算手段は、前記平文及び前記第1付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第2付加情報を削除して復号文を生成する。この構成によると、前記可逆演算手段は、前記平文及び前記第1付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第2付加情報を削除して復号文を生成するので、前記復号結合情報から確実に復号文を生成することができる。

【図面の簡単な説明】

【図1】暗号通信システム1の構成を示すブロック図である。

【図2】暗号化部105の構成を示すブロック図である。

【図3】復号化部202の構成を示すブロック図である。

【図4】送信装置10の動作を示すフローチャートである。図5に続く。

【図5】送信装置10の動作を示すフローチャートである。図4から続く。

【図6】受信装置20の動作を示すフローチャートである。

【図7】算出方法6において用いられる変換テーブルの一例を示す。

【図8】暗号通信システム1の第1の変形例としての暗号通信システム1bの構成を示すブロック図である。

【図9】暗号通信システム1bの動作を示すフローチャートである。

【図10】暗号通信システム1の第2の変形例としての暗号通信システム1cの構成を示すブロック図である。

【図11】暗号通信システム1cの動作を示すフローチャートである。

【図12】暗号通信システム1の第3の変形例としての暗号通信システム1dの構成を示すブロック図である。

【図13】暗号通信システム1dの動作の動作を示すフローチャートである。



【図14】変形例の実現可能な組合せを示す表である。

【符号の説明】

1 暗号通信システム

10 送信装置

20 受信装置

30 インターネット

101 平文記憶部

102 付加情報生成部

103 情報付加部

104 一方向性関数部

105 暗号化部

106 送信部

201 受信部

202 復号化部

203 情報除去部

204 一方向性関数部

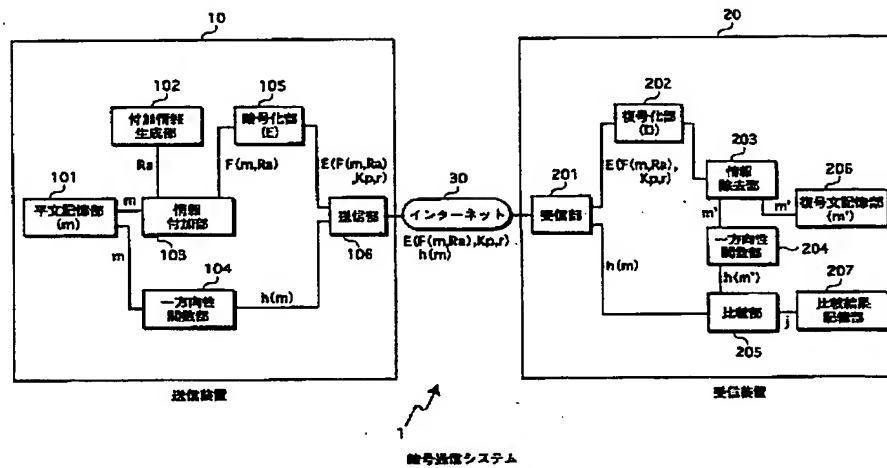
205 比較部

206 復号文記憶部

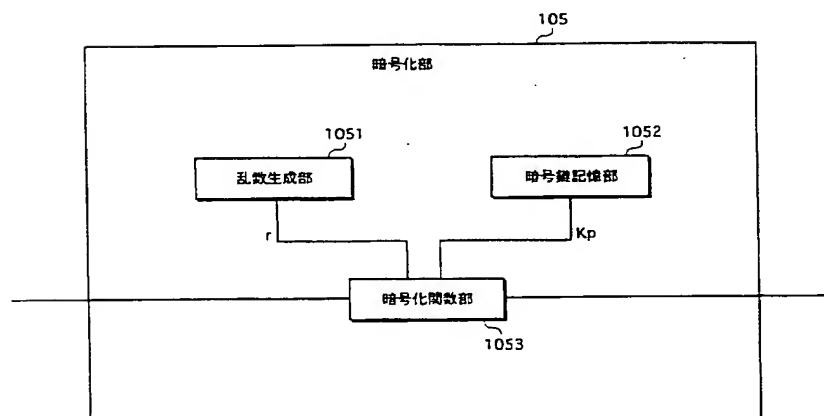
207 比較結果記憶部

10 209 付加情報生成部

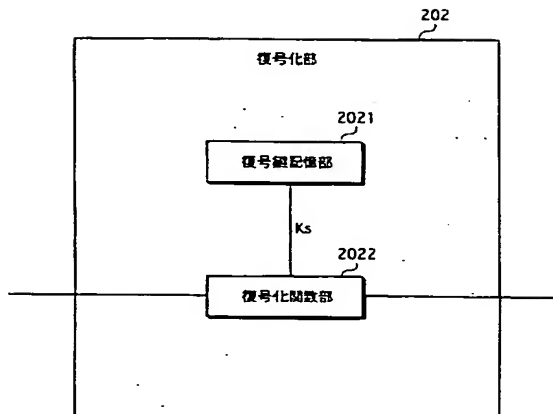
【図1】



【図2】



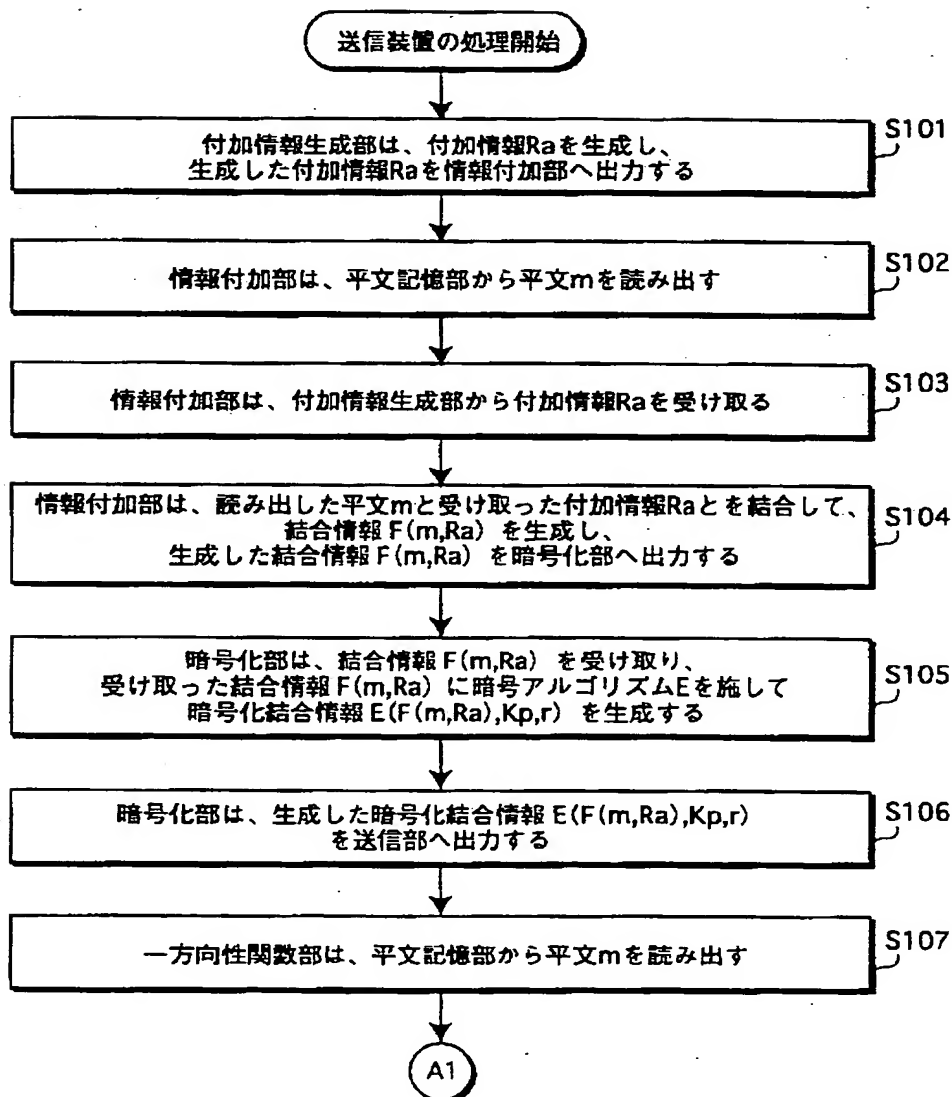
【図3】



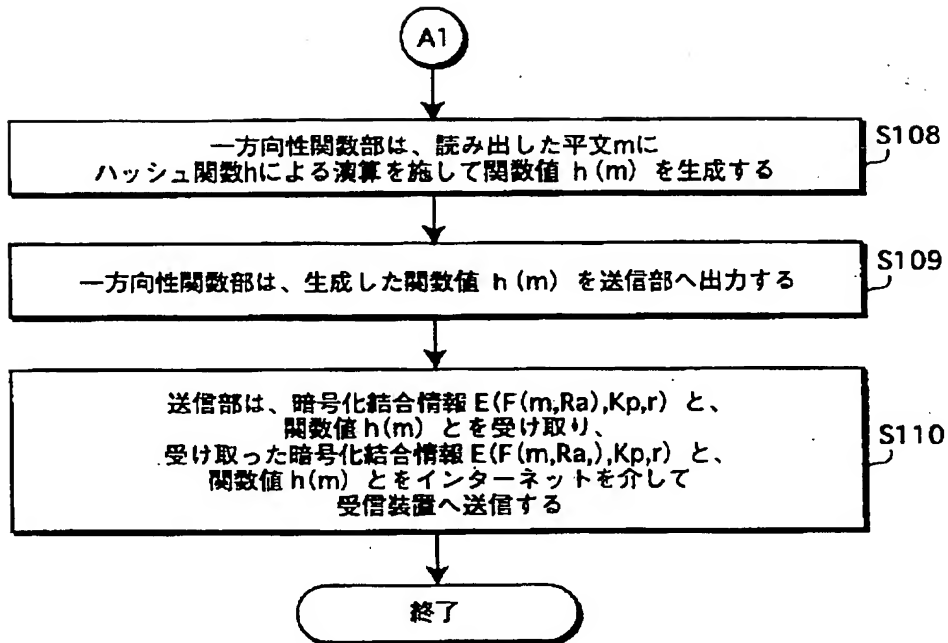
【図14】

付加情報	(1) Ra: 乱数	(2) Ra: タイムスタンプ	(3) Ra: カウンタ
可逆変換 $F(m, Ra)$	暗号通信システム 1, 1b~1d		
(1) $m \parallel Ra$	暗号通信システム 1b~1d		
(2) $m \oplus Ra$			
(3) $m + Ra$			
(4) $m \times Ra \bmod p$			
(5) $\text{BitPerm}[Ra](m)$			
(6) $\text{Tab}[Ra](m)$			

【図4】



【図5】

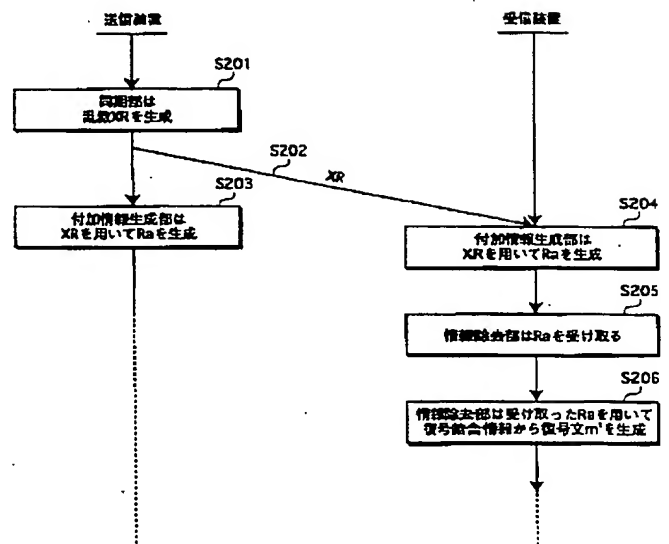


【図7】

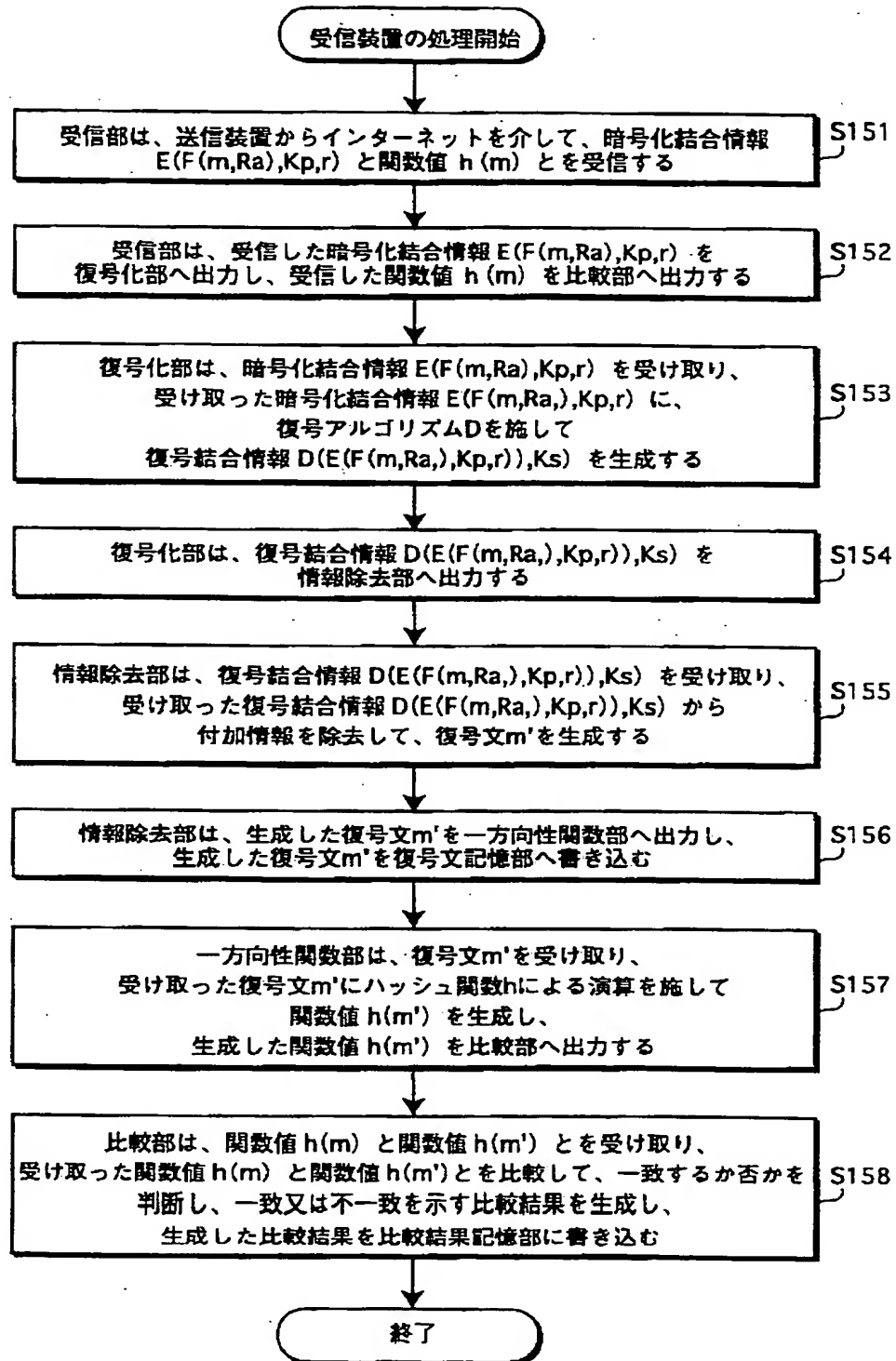
変換テーブル

入力値m	出力値 Tab[Ra](m)
0	122
1	39
⋮	⋮
255	91

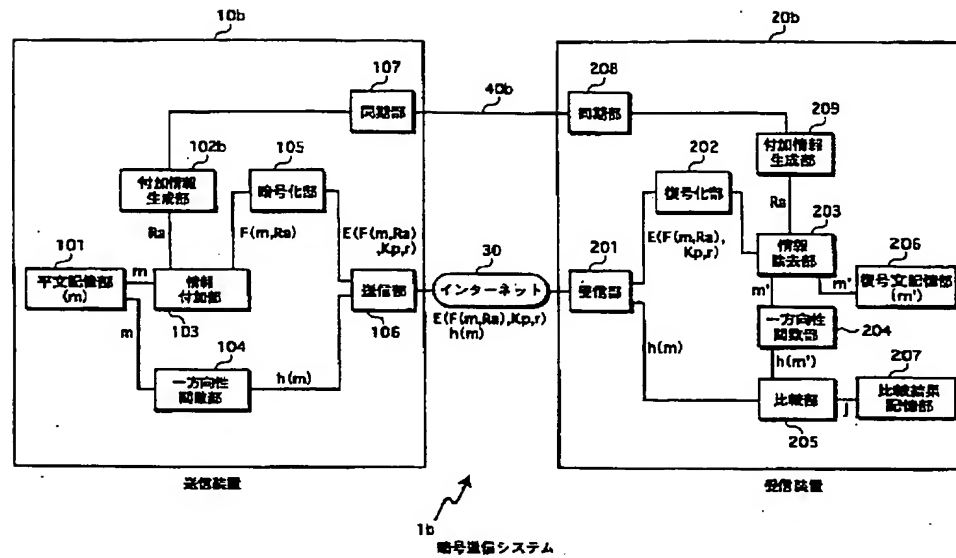
【図9】



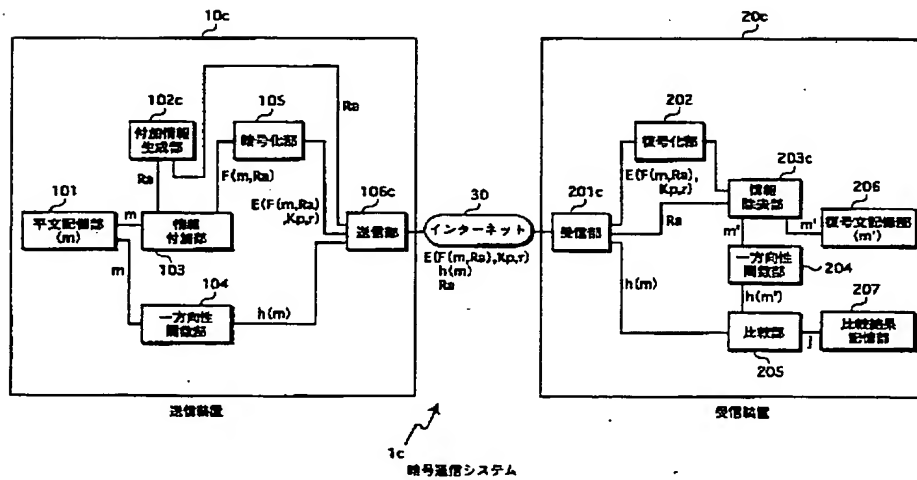
【図6】



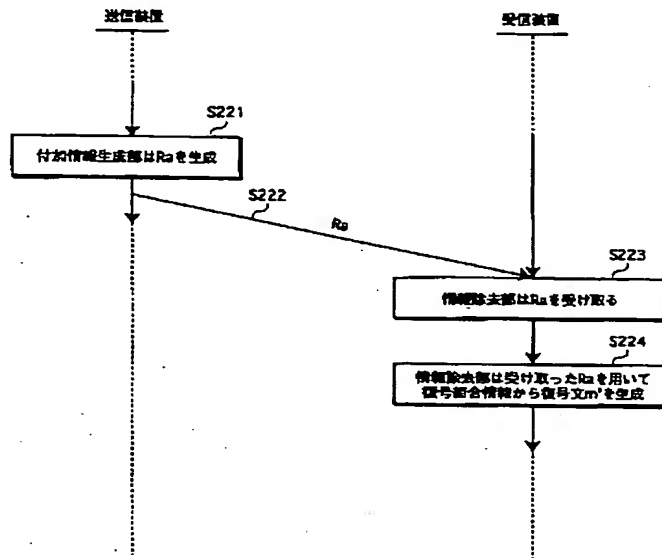
【図 8】



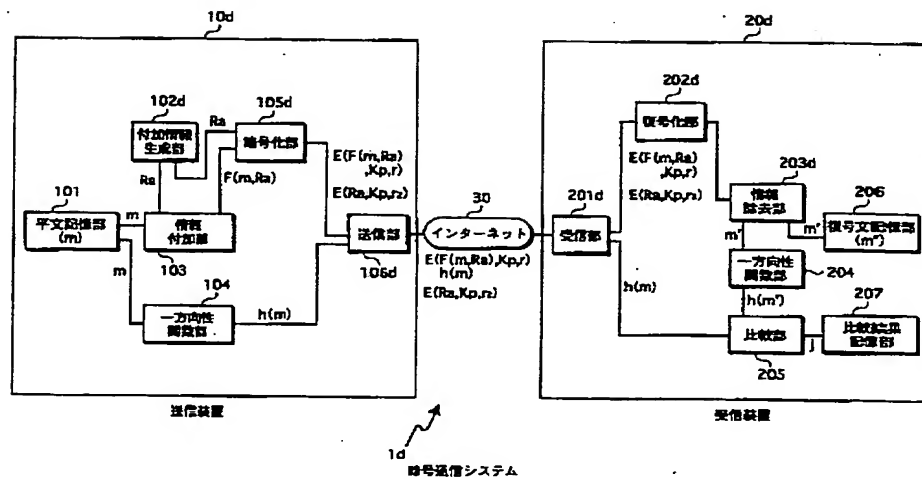
【図 10】



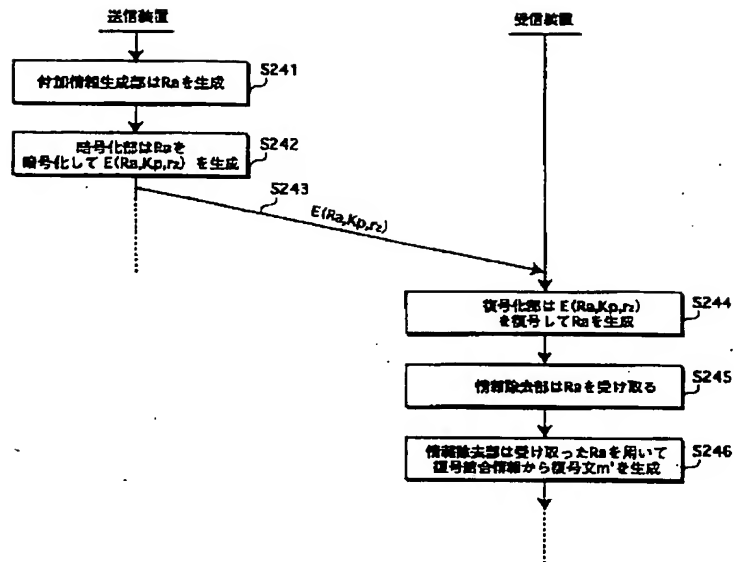
【図11】



【図12】



【図13】



フロントページの続き

(72)発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 5J104 AA28 FA07 JA04 NA11

**THIS PAGE BLANK (USPTO)**